DEPARTM

National Highway Traffic Safety Administration

[Docket No. NHTSA-2020-0087]

Cybersecurity Best Practices for the Safety of Modern Vehicles

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT).

ACTION: Notice of federal guidelines.

SUMMARY: On January 12, 2021, NHTSA released its draft *Cybersecurity Best Practices for the Safety of Modern Vehicles* guidance ("Draft Best Practices" or "guidance") in an effort to support industry-led efforts to improve the industry's cybersecurity posture as well as provide NHTSA's views on how the automotive industry can develop and apply sound, risk-based cybersecurity management processes during the vehicle's entire lifecycle. These guidelines are intended to be applicable to all individuals and organizations involved in the design, development, manufacture and assembly of a motor vehicle and its electronic systems and software. These entities include, but are not limited to, small and large-volume motor vehicle and motor vehicle equipment designers, suppliers, manufacturers, and modifiers. This document summarizes comments received in response to the draft guidance, responds to those comments, and describes changes made to the draft guidance in response to those comments. This document also announces the issuance of the final version of the *Cybersecurity Best Practices for the Safety of Modern Vehicles* guidance. While this is the final version of this iteration of the Best Practices, NHTSA routinely assesses cybersecurity risks as well as emerging best practices and will consider future updates as motor vehicles and their cybersecurity evolve.

DATES: The changes made in this document are effective upon publication.

FOR FURTHER INFORMATION CONTACT: For technical issues, please contact Mr. John I. Martin of NHTSA's Office of Vehicle Safety Research at 937-366-3246 or

john.martin@dot.gov. For legal issues, contact Ms. Sara R. Bennett of NHTSA's Office of Chief Counsel at 202-366-2992 or sara.bennett@dot.gov.

SUPPLEMENTARY INFORMATION: This final version of the Cybersecurity Best Practices for the Safety of Modern Vehicles does not have the force and effect of law and is not a regulation. This guidance document will not be published in the Code of Federal Regulations but will be posted on NHTSA's website, www.nhtsa.gov.

I. Introduction

In January 2021, NHTSA released its draft *Cybersecurity Best Practices for the Safety of Modern Vehicles* guidance document ("Draft Best Practices" or "guidance") with the goal of supporting industry-led efforts to improve the industry's cybersecurity posture and provide the Agency's views on how the automotive industry can develop and apply sound, risk-based cybersecurity management processes during the vehicle's entire lifecycle. As background, the Draft Best Practices document is an update to NHTSA's first cybersecurity best practices document, *Cybersecurity Best Practices for Modern Vehicles* ("2016 Best Practices"). NHTSA requested comment on the Draft Best Practices in an accompanying Federal Register notice.[1]

The Draft Best Practices builds upon agency research and industry progress since 2016, including emerging voluntary industry standards, such as the International Organization for Standardization (ISO)/SAE International (SAE) Draft International Standard (DIS) 21434, "Road Vehicles—Cybersecurity Engineering."[2] In addition, the Draft Best Practices references a series of industry best practice documents developed by the Automotive Information Sharing and Analysis Center (Auto-ISAC) through its members. The Draft Best Practices also reflects findings from NHTSA's continued research in motor vehicle cybersecurity, including over-the-air updates, formal verification, static code analysis, new learnings obtained through researchers and stakeholder engagement as well as continued building of our capability in cybersecurity

[1] 86 FR 2481 (Jan. 12, 2021).
[2] ISO/SAE 21434:2021 Road Vehicles—Cybersecurity Engineering, available at: https://www.iso.org/standard/70918.html.

testing and diagnostics. The updates included in the Draft Best Practices incorporate insights gained from public comments received in response to the 2016 guidance and from information obtained during the annual SAE/NHTSA Vehicle Cybersecurity Workshops.

The Draft Best Practices touches on a wide array of issues associated with safety-related cybersecurity practices, and provides recommendations to industry on the following topics:

- General Cybersecurity Best Practices
- Education
- Aftermarket/User-Owned Devices
- Serviceability
- Technical Vehicle Cybersecurity Best Practices

The first topic in the list, "General Cybersecurity Best Practices," is the largest topic and discusses cybersecurity practices with respect to industry stakeholders. There are a variety of practices in this category. For example, one practice suggests that manufacturers should evaluate all commercial off-the-shelf and open-source software components used in vehicle Electronic Control Units (ECUs) against known vulnerabilities.[3]

The second topic, "Education," discusses the role and responsibilities of industry and academia in supporting an educated cybersecurity workforce.

The third topic, "Aftermarket/User-Owned Devices," discusses the issues associated with connecting aftermarket devices to vehicle systems. For instance, the guidance suggests that any connection to a third-party device should be authenticated and provided with appropriate, limited access.[4]

The fourth topic, "Serviceability," touches on industry's obligation to simultaneously provide for both cybersecurity and third-party serviceability.

[3] G.12 in NHTSA's Cybersecurity Best Practices for the Safety of Modern Vehicles.
[4] G.42 in NHTSA's Cybersecurity Best Practices for the Safety of Modern Vehicles.

The last topic, "Technical Vehicle Cybersecurity Best Practices," discusses cybersecurity practices with respect to the vehicle. As an example, one of the 25 technical vehicle cybersecurity best practices suggests that network segmentation and isolation techniques should be used to limit connections between wireless-connected ECUs and low-level vehicle control systems, particularly those controlling safety critical functions, such as braking, steering, propulsion, and power management.

This notice summarizes the comments received, NHTSA's responses to those comments, and finalizes the Draft Best Practices document. The final Best Practices document continues to use the numbering scheme introduced in the Draft Best Practices document. For example, it uses [G.1] through [G.45] for general cybersecurity best practices and [T.1] through [T.25] for technical vehicle cybersecurity best practices. Additions to the Draft Best Practices mean that there are some numbering differences between the draft and final versions of the Best Practices. This Federal Register notice exclusively refers to the final Best Practices numbering scheme, rather than the draft version. Cases where there are differences between the draft and final numbering scheme are noted with a footnote. Finally, the agency stresses that the final Best Practices remain voluntary and non-binding, as has been the case with this guidance beginning with its initial 2016 edition.

II. Summary of Differences Between the Draft and Final Cybersecurity Best Practices for the Safety of Modern Vehicles

The purpose of this section is to provide a summary of the differences between the draft and final Cybersecurity Best Practices for the Safety of Modern Vehicles. The next section of this document, "Summary of Public Comments Received in Response to Draft Cybersecurity Best Practices," will discuss the comments received and the reasons why these changes were made.

The following provides a high-level summary of changes made in the final version. First, in response to a comment, NHTSA clarified, with a minor edit, that the scope of the Best

Practices includes all individuals and organizations involved in the maintenance of a motor vehicle. Second, the Agency updated all references to the ISO/SAE 21434 standard to reflect the finalized version of the subject industry standard, which occurred after the Draft Best Practices were published for comments. Third, in the General Cybersecurity Best Practices section, several headings were retitled in response to comments, and the new changes clarified terms, and altered the order of mention of the Auto-ISAC and standards development organizations (SDO) in some places to avoid unintended potential referencing to Auto-ISAC as an SDO. Additionally, NHTSA added a new general cybersecurity best practice to address future risks and bifurcated an existing one into two separate practices based on well-supported comments. Fourth, in the Technical Cybersecurity Best Practices section, NHTSA added mention of current cryptographic techniques and their implementation and made wording changes to clarify protections from unauthorized disclosure and accessibility to other vehicles. The Agency also added a new technical practice to limit firmware version rollback attacks and rewrote a technical practice [T.11].[5] The new practice now reads "[T.11][6] Employ best practices for communication of critical information over shared and possibly insecure channels. Limit the possibility of replay, integrity compromise, and spoofing. Physical and logical access should also be highly restricted." Fifth, NHTSA added definitions of "global symmetric keys" and "recovery" to the appendix's Terms and Descriptions section. Finally, NHTSA updated and added minor wording changes and references throughout, including addressing clerical errors.

III. Summary of Public Comments Received in Response to Draft Cybersecurity Best Practices

NHTSA received comments from a total of 38 entities in response to the Draft Best Practices, published in January 2021. These comments came from government entities,[7] industry

[5] In the draft version, this was T.10.
[6] In the draft version, this was T.10.
[7] California Highway Patrol.

associations,[8] standards development organizations,[9] automotive and equipment manufacturers,[10] consumer and safety advocacy organizations,[11] university and research organizations,[12] and individuals.[13] The comments represent an evolution of vehicle cybersecurity opinion among stakeholders and the general public. Comments to the 2016 guidance tended to be general and higher-level (i.e., bigger-picture). In contrast, comments received in response to the Draft Best Practices focused on discrete issues important to commenters. This evolution is also likely due to the introduction of vehicle-specific cybersecurity standards and best practices in the automotive sector. Overall, most commenters seemed supportive of NHTSA's efforts to encourage continual progress in the automotive sector through the issuance of best practices, though there was some divergence as to the details of what those best practices should contain, the level of detail necessary to fulfill the agency's goals, and other specific topics commenters stated NHTSA should address. The aggregated comments presented several high-level themes, and thus, this document presents comments organized by the following categories of request:

- More specifics in the guidance;
- Industry collaboration;
- Minor editorial amendments;
- Additional references to ISO/SAE 21434;
- Additional references to other standards;
- Clarification of entity designations;
- Changes in scope; and

[8] Alliance for Automotive Innovation, American Alliance for Vehicle Owner's Rights, American Trucking Association, Auto Care Association, Automotive Aftermarket Suppliers Association, Automotive Recyclers Association, Specialty Equipment Market Association, National Motor Freight Traffic Association, National Automobile Dealers Association, Motor Equipment Manufacturers Association and Consumer Technology Association.
[9] SAE and Institute of Electrical and Electronics Engineers.
[10] General Motors LLC, Toyota Motor Corporation, Continental Automotive Systems, Denso Corporation, ZF North America, Robert Bosch GmbH, Amazon Web Services, Blackberry Corporation, AT&T, GeoTab, Nuro, Arilou Automotive Cybersecurity and LKQ Corporation.
[11] Center for Auto Safety, Privacy4Cars, SecuRepairs and Digital Right to Repair Coalition.
[12] Carnegie Mellon Software Engineering Institute, Sandia National Laboratories, Underwriters Laboratories LLC.
[13] Norman Field, Rik Farrow,Ryan Moss and Howard Hoffman.

- Right to repair.

In the sections that follow, NHTSA summarizes each category of major comments received in response to the Draft Best Practices and the agency's response.

a. Commenter requested more specifics in the guidance

Several commenters requested that NHTSA make certain language in the guidance more specific to address issues important to the commenter. As background, NHTSA intends to maintain wide applicability in the Draft Best Practices, so that it can encompass the many industry stakeholders, variety of business models, and vehicle and equipment architectures available on the market. This guidance is also intended to be flexible enough to encompass future business models and vehicle and equipment designs, to help ensure that this guidance remains helpful and relevant beyond a single point in time. Even so, NHTSA found it possible to integrate several suggestions from commenters in response to requests for more specificity. As such, NHTSA added two definitions to the document's glossary, and made the changes described below.

The two definitions that NHTSA added in response to comments are for the terms, "recovery," and "global symmetric keys." The Institute of Electrical and Electronics Engineers (IEEE), a standards setting professional organization, suggested defining the term "recovery" in the context of referencing the National Institute of Standards and Technology (NIST) Cybersecurity Framework's five principal functions "Identify, Protect, Detect, Respond and Recover." IEEE suggested that the document did not describe what was meant by "recovery." Toyota Motor Corporation (Toyota) and Geotab suggested defining the specific term "global symmetric keys" because, in their opinion, the meaning may not be obvious. NHTSA considered the merits of adding these new definitions for improving clarity and agreed that their addition would be beneficial for public understanding, and thus, added them to the final Best Practice's appendix in "Terms and Definitions".

In section 8.2 of the Draft Best Practices, "Cryptographic Credentials," Sandia National Laboratories (Sandia) and DENSO Corporation (Denso) suggested additional specific discussion of cryptographic techniques and standards. In response, NHTSA has modified section 8.2 with additional text and a slight title change that reflects section 8.2's new focus on techniques.

Sandia also expressed the comment that, "The claim that Public key cryptography techniques are more secure than symmetric key systems should be caveated with 'properly implemented techniques' are 'generally' more secure….".[14] While Sandia made this comment with respect to section 8.3 of the Draft Best Practices, "Vehicle Diagnostic Functionality," NHTSA responded to Sandia's comment by incorporating the text "While the selection of appropriate cryptographic techniques is an important design criterion, it should be noted that implementation issues often determine any system's security" into section 8.2. NHTSA considered Sandia's assertion to be correct, and NHTSA agrees that implementation issues are very important.

NHTSA also incorporated a comment from SAE that asked for technical guidance that would limit firmware version rollback attacks where an attacker may use software update mechanisms to place older, more vulnerable software on a targeted device. NHTSA agrees that the practice of manufacturers allowing the installation of older, potentially vulnerable versions of firmware in vehicles and vehicle equipment should be avoided whenever possible. In response, NHTSA added practice [T.23].

Because of NHTSA's desire for the document to remain broadly applicable, many comments asking for additional specifics were not incorporated into the guidance. For instance, NHTSA did not accept comments suggesting that the agency explicitly define terms such as "lifecycle," "end-of-life," and "state of the art," among others. NHTSA acknowledges that many of these terms may have different meanings to different companies and stakeholders, but

[14] See Comment ID "NHTSA-2020-0087-0009" for Document "NHTSA-2020-0087-0002" on the regulations.gov web site.

NHTSA did not believe it would be appropriate to define these terms in such a way that might inadvertently suggest limitations to or conflicts with company responsibilities, such as manufacturers' responsibility to notify NHTSA of any safety defect in its motor vehicles or motor vehicle equipment.[15]

Similarly, while NHTSA encourages companies to pay close attention to cybersecurity throughout its corporate structures and supply chain, NHTSA does not view this guidance as a mechanism to suggest how corporate responsibilities among companies should be distributed. This guidance does not attempt to provide any particular view of the automotive supply chain, and NHTSA recognizes that many of these considerations may be handled via contract. Although ISO/SAE 21434 does address supply chain responsibilities to some extent, NHTSA's Best Practices purposefully does not provide such details.

In other cases of requested specificity, NHTSA determined that some commenters' requests inadvertently resulted in limiting the applicability of the document. As stated before, one of NHTSA's underlying goals of this document was to ensure it remains accessible to a wide audience and all of NHTSA's regulated entities.

NHTSA also tries to maintain the document's generality by limiting language specific to a particular corporate process, perhaps even specific to a particular corporation. Comments that make suggestions encompassing specific corporate processes have not been incorporated into the updated document.

In addition, a comment asked NHTSA to address forensic data retrieval. NHTSA recognizes the importance of forensic data retrieval but has determined that the subject is out-of-scope for this document.

b. Commenter encourages industry collaboration

Many commenters expressed the sentiment that industry collaborative efforts are a good idea, including the Alliance for Automotive Innovation (Alliance) and Amazon Web Services

[15] 49 U.S.C. 30118(c).

(Amazon), both of which provided specific comments encouraging collaboration. The Alliance suggested that NHTSA create a new section on emerging risks where there may not be established best practices developed to manage those risks. The Alliance suggested that this new section should include high-level recommendations to encourage industry-wide collaboration to establish best practices to treat those risks. Amazon suggested NHTSA should encourage industry collaboration to identify attempted and successful exploitations and attacks not previously considered in the design and assessment phases.

NHTSA agrees with the importance of industry collaboration, especially within the automotive cybersecurity realm. Therefore, NHTSA has encouraged membership and active participation in the Auto-ISAC and collaboration through its annual cybersecurity forum that the agency holds with SAE. In response to these commenters, NHTSA added a new general practice [G.24] that states: "As future risks emerge; industry should collaborate to expediently develop mitigation measures and best practices to address new risks." NHTSA believes that this addition and the rest of the guidance covers both commenters' suggestions.

c. Commenter requested minor editorial amendments

Many commenters provided a wealth of suggested additional word choices, terminology changes, and phrasing modifications. NHTSA appreciates these suggestions and adopted these changes wherever possible and is grateful for the improvements these suggestions provide.

Multiple comments[16] pointed out a typographical error in section 4.5 where "[G.27[a]-[c]]"[17] should have been "[G.28[a]-[c]."[18] NHTSA adopted the suggested change. Other editorial amendments include modifying the word "standards" in [G.9] to "expectations." In the draft Best Practices, [G.9] stated "Clear cybersecurity standards should be specified and communicated to the suppliers that support the intended protections." NHTSA adopted the change to the word "expectations" because commenters suggested they needed additional clarification as to what

[16] ZF North America, Arilou Automotive Cybersecurity, National Motor Freight Traffic Administration.
[17] In the draft version, this was G.26.
[18] In the draft version, this was G.27.

word “standards” means in that particular practice. NHTSA believes “expectations” would maintain the agency’s intended breadth while also clarifying any ambiguity for stakeholders.

Another commenter suggested that NHTSA remove “that” from “NHTSA recommends that:” in section 4.3 of the Draft Best Practices. NHTSA adopted this edit accordingly.

Some commenters suggested changes to section titles to add additional clarity for stakeholders. In two instances, NHTSA adopted those suggestions to change section titles. Section 4.2.7 was originally titled “Penetration Testing and Documentation” in the draft guidance and is now titled “Cybersecurity Testing and Vulnerability Identification” in the final guidance. NHTSA felt that the new title was appropriately general. Similarly, section 4.2.4 was originally titled “Unnecessary Risk Removal” and is now “Removal or Mitigation of Safety-Critical Risks.” The new title better describes the section.

SAE suggested changes to [T.4][19] that changed the existing text to “Cryptographic credentials that provide an authorized, elevated level of access to vehicle computing platforms should be protected from unauthorized disclosure or modification”. NHTSA welcomes this change because it additionally emphasizes the consequences of modifying platform credentials.

Several commenters recommended minor amendments to [T.5][20] “Any credential obtained from a single vehicle’s computing platform should not provide access to multiple vehicles.” The technical guidance now reads “other vehicles” rather than “multiple vehicles” as was included in the draft guidance. NHTSA feels that the use of the word “other” more clearly focuses the issues involved in using universally applicable credentials.

National Motor Freight Traffic Association (NMFTA) recommended minor amendments to general practice [G.6] “Manufacturers should consider the risks associated with sensor vulnerabilities and potential sensor signal manipulation efforts such as GPS spoofing, road sign modification, Lidar/Radar jamming and spoofing, camera blinding, or excitation of machine

[19] In the draft version, this was T.3.
[20] In the draft version, this was T.4.

learning false positives." The general guidance now reads "…camera blinding, and excitation…" rather than "…camera blinding, or excitation…." NHTSA agrees with NMFTA's comment that the use of "or" rather than "and" incorrectly suggests that manufacturers could focus on any one of the presented spoofing issues rather than considering all the spoofing issues.

SAE suggested that [G.10] needed to focus on hardware and software rather than just software. In the Draft Best Practices, general practice [G.10] stated "Manufacturers should maintain a database of operational software components used in each automotive ECU, each assembled vehicle, and a history log of version updates applied over the vehicle's lifetime." NHTSA agrees that software inventory management alone is not sufficient and made changes to [G.10] to include a discussion of inventory management of both hardware and software. Robert Bosch GmbH (Bosch) additionally suggested that the subject of [G.10] needed to be "Suppliers and vehicle manufacturers" rather than "Manufacturers." NHTSA agrees with the change because it maintains the desired generality while directing the reader to specific entities.

In the Draft Best Practices, general practice [G.30][21] stated "Organizations should document the details of each identified and reported vulnerability, exploit, or incident applicable to their products. These documents should include information from onset to disposition with sufficient granularity to support response assessment." Underwriters Laboratories (UL) suggested rephrasing the second sentence as: "The nature of the vulnerability and the rationale for how the vulnerability is managed should also be documented." NHTSA agrees that UL's suggested wording is an improvement. NHTSA also felt that [G.30][22] could be better expressed as two separate general practices and made a new general practice to reflect UL's wording.

SAE suggested changes to [G.41][23] in the Draft Best Practices, which stated "The automotive industry should consider the incremental risks that could be presented by these devices when connected with vehicle systems and provide reasonable protections." The

[21] In the draft version, this was G.29.
[22] In the draft version, this was G.29.
[23] In the draft version, this was G.39.

commenter suggested removing the word "incremental," changing "automotive industry" to "automotive manufacturers," and changing "these devices" to "user owned or aftermarket devices." NHTSA declines to change "automotive industry" to "automotive manufacturers" because the goal of this guidance document is to retain broad utility for the entire automotive industry, not just manufacturers. NHTSA agreed to remove the word "incremental" from the general practice and to replace the term "these devices" with a more accurate phrase, "user owned or aftermarket devices."

In the Draft Best Practices, [T.11][24] stated "Critical safety messages, particularly those passed across non-segmented communication buses, should employ a message authentication method to limit the possibility of message spoofing." SAE felt that [T.11][25] needed to be reworded as: "Employ best practices for communication of critical information over shared and possibly insecure channels. Limit the possibility of replay, integrity compromise, and spoofing. Physical and logical access should also be highly restricted." NHTSA adopted SAE's suggested language for technical practice because the new wording expresses more general guidance than the draft version while encompassing the draft version's meaning.

There were many other suggestions for minor wording or phrasing changes that NHTSA considered. NHTSA adopted those that would not change the underlying intent of that particular section of the guidance document, but many suggestions from commenters would have worked to either limit or narrow the scope of the guidance. As such, those suggestions were not adopted since they would be contrary to the intent and goals of this document.

d. Commenter requested additional references to ISO/SAE 21434

ISO/SAE 21434 is a newly developed standard titled "Road Vehicles – Cybersecurity Engineering."[26] This standard serves as an overarching industry consensus standard for vehicle

[24] In the draft version, this was T.10.
[25] In the draft version, this was T.10.
[26] ISO/SAE 21434:2021 *Road vehicles – Cybersecurity engineering*, available at: https://www.iso.org/standard/70918.html and https://www.saemobilius.sae.org.

cybersecurity, and it is extensively referenced in NHTSA's "Cybersecurity Best Practices for the Safety of Modern Vehicles." Many commenters pointed out that NHTSA referenced the earlier Draft International Standard (DIS) version of ISO/SAE 21434, and suggested that NHTSA needed to update the references in the final Best Practices to the final ISO/SAE 21434 version, which was due to be released in Fall 2021. NHTSA followed this advice. In the final Best Practices, NHTSA has changed the latest the guidance to reflect the content of the latest "FDIS" or "Final Draft International Standard" version of ISO/SAE 21434.

While NHTSA extensively referenced ISO/SAE 21434, the commenters pointed out areas where NHTSA could have included a reference to a relevant section of ISO/SAE 21434 and did not. As an example, commenters pointed out that [G.12] and [G.37][27] could refer to the relevant clauses of ISO/SAE 21434. NHTSA adopted these suggestions and added a reference to ISO/SAE 21434 clause 6 in [G.12]. General practice [G.37][28] now references requirements in clauses 5 and 6 of ISO/SAE 21434. Another commenter corrected NHTSA's reference to ISO/SAE 21434 in a footnote to general practice [G.16]. NHTSA accepted that correction.

NHTSA also included the website https://www.saemobilius.sae.org as a source for ISO/SAE 21434 in addition to the previously referenced https://www.iso.org.

e. Commenter requested additional references to other standards

Another category of comments requested that NHTSA provide new references to additional source material that were favored by the commenter. In many cases, NHTSA was able to incorporate these suggestions. NHTSA added only those references and referenced materials that the agency found were: (1) Sufficiently high level; (2) Specific to automotive industry or could be obviously applied to the automotive industry; (3) Not under development; and/or (4) Not duplicative of information or references already included in the Draft Best Practices.

[27] In the draft version, this was G.35.
[28] In the draft version, this was G.35.

For example, one commenter stated that NHTSA should add references to the NIST cryptography standards to supplement technical practice [T.4][29], dealing with cryptographic credentials. NHTSA decided that this modification met the criteria described above, and the agency adopted this suggestion by adding a technical practice [T.3] and a reference to NIST's Federal Information Processing Standards (FIPS) 140 Series. The FIPS 140 series is a set of documents updated by NIST that describes minimum standards for cryptography.

Another commenter stated that NHTSA should reference ISO 24089 "Road vehicles – Software update engineering" in the Best Practices. NHTSA did not incorporate this comment because ISO 24089 is under development at this time. NHTSA may revisit this decision in future iterations of its cybersecurity best practices after ISO 24089 is finalized.

NMFTA requested that NHTSA reference the Cybersecurity and Infrastructure Security Agency's (CISA's) binding operational directive 20-01 in general practice [G.27]'s[30] discussion of vulnerability reporting. NHTSA agreed with this change and felt that it provided support for the guidance.

In response to a comment from SAE, NHTSA also added a reference to a NIST white paper titled "Mitigating the Risk of Software Vulnerabilities by Adopting a Secure Software Development Framework (SSDF)" for general practice [G.22], dealing with best practices for secure software development.

Responding to a comment from NMFTA, NHTSA added a footnote reference to the SAE CyberAuto Challenge and the Cyber Truck Challenge as examples for general practice [G.40][31], dealing with educational efforts targeted at workforce development in the field of automotive cybersecurity. NHTSA also used this additional footnote to call out NHTSA's efforts to fund and develop cybersecurity curricula.

---

[29] In the draft version, this was T.3.
[30] In the draft version, this was G.26.
[31] In the draft version, this was G.38.

Other commenters requested that NHTSA add in references to the World Forum for Harmonization of Vehicle Regulation's (WP.29) United Nations (UN) Regulation 155 – "Cyber security and cyber security management system." In most cases, the public comments recommended high-level alignment, without further specifying the sources of potential misalignment that may have been a concern. UN ECE 155 is a type-approval regulation[32] that establishes not only recommended practices but also sufficiency standards for approval. Standards for type approval are well beyond the scope and intent of NHTSA's Best Practices document. Therefore, NHTSA did not explicitly reference the UN ECE 155. NHTSA could revisit this topic in future iterations based on more specific public feedback.

f. Commenter requested clarification of entity designations

Several comments pointed out that the NHTSA's Cybersecurity Best Practices seemed to falsely suggest that the Auto-ISAC is a standard setting organization (SSO). NHTSA has modified general practices [G.18] and [G.23] in an effort to correct this impression. Even so, these modifications should not be interpretated as anything more than textual clarifications. The modifications do not represent any change in NHTSA's position that guidance to industry, whether from a SSO or not, can be valuable to encourage progress in cybersecurity practices of the automotive industry.

g. Commenters requested changes in scope

Many commenters requested a variety of changes in scope for the Draft Best Practices. Commenters diverged in their requests for changes to the scope. NHTSA did not incorporate most of the requested scope changes because NHTSA carefully considered the scope of the Draft Best Practices document at the development and drafting stages, and NHTSA believes that the

[32] UN ECE 155 is a regulation established under the United Nations Economic Commission for Europe (UNECE) 1958 Agreement concerning the Adoption of Uniform Technical Prescriptions for Wheeled Vehicles, Equipment and Parts which can be Fitted and/or be Used on Wheeled Vehicles and the Conditions for Reciprocal Recognition of Approvals Granted on the Basis of these Prescriptions (*Available at* https://unece.org/trans/main/wp29/wp29regs), and the United States is not party to this agreement. Further, UN Regulation 155 is a regulation for type approving authorities, and the United States is not a country that engages in type approval of motor vehicles or motor vehicle equipment.

existing scope of the document is most compatible with its mission and goals for this document. For example, narrowing the scope might imply inaccurately that NHTSA does not intend this guidance to be useful to all its regulated entities, and broadening the scope might exceed the agency's intended audience.

While most comments concerning the document's scope were not incorporated, NHTSA responded to the National Automobile Dealers Association's comments concerning the critical role of automotive dealers by adding the word "maintenance" to the following text of the Scope, which was an explicit clarification that scope includes that function: "Importantly, all individuals and organizations involved in the design, manufacturing, assembly and maintenance of a motor vehicle have a critical role to play with respect to vehicle cybersecurity."

Many commenters felt that NHTSA needed to address heavy trucks more explicitly and directly, but NHTSA believes this would be unnecessary since the scope of the Draft Best Practices already includes heavy trucks.

Other commenters felt that NHTSA needed to more explicitly address vehicles equipped with Automated Driving Systems (ADS), asserting that these vehicles would have cybersecurity needs much different from modern vehicles. NHTSA believes that the underlying technical sources of cybersecurity vulnerabilities as well as risk-based approaches and toolsets to address them are unlikely to be substantially different for vehicles equipped with ADS. Therefore, at the levels of guidance included, the Draft Best Practices already covers vehicles equipped with ADS, and NHTSA believes that any more specificity for ADS is unnecessary at this time. However, the Agency believes that the societal risk tolerance associated with cybersecurity risks for vehicles equipped with ADS may be significantly lower than for traditional vehicles, and, thus, the Agency will continue to monitor factors around these recommendations with incoming research results and consider them in future updates.

Some commenters stated that NHTSA should explicitly address enterprise information technology (IT) issues. While NHTSA agrees that enterprise IT security is an important topic,

NHTSA specifically avoided making suggestions regarding internet infrastructure that do not directly touch vehicles. NHTSA recognizes that a hypothetical situation, such as the theft of vehicle code signing keys from a poorly secured, internet-connected server, could be an example of an enterprise IT security issue that could impact a vehicle. However, as part of this document's scope, NHTSA focuses primarily on those cybersecurity issues that directly impact vehicles, and thus occupant and road user, safety. In addition to cybersecurity safety issues, NHTSA is invested in vehicle theft prevention and engages in activities to reduce motor vehicle theft through its Vehicle Theft Prevention Program.

Another set of commenters requested that NHTSA expand the scope of the Draft Best Practices to address a variety of consumer privacy issues. Many of these commenters indicated that they believed that a substantial part of cybersecurity implicates privacy and privacy cannot be separated from cybersecurity. In this vein, some comments suggested that NHTSA needed to address a concept called the confidentiality, integrity, and availability triad, aka "CIA triad."[33] While NHTSA agrees about the general importance of the topic of consumer confidentiality, NHTSA's Best Practices retains its intended focus on cybersecurity, particularly those cybersecurity issues that could impact the safety of the vehicle or equipment safety. NHTSA believes this focus most closely aligns with its safety mission. We believe privacy issues can and should be addressed elsewhere.

Finally, many commenters expressed concern that NHTSA's Cybersecurity Best Practices focused on the automotive industry at the expense of advising the consumer. NHTSA's intended audience for the Best Practices is the regulated industry. The primary responsibility for vehicle and equipment safety, including that of vehicle software and any cybersecurity protections applied, is industry, and NHTSA retains this focus in the final version. NHTSA is interested in consumer education topics, but the agency believes that an educated consumer

[33] https://en.wikipedia.org/wiki/Information_security.

provides an additional layer of protection that does not change the best practices recommendations to the automotive industry.

h. Right to repair

Many comments discussed right-to-repair issues. Some of the right-to-repair comments suggested that NHTSA assign software rights to various parties. As stated in the Draft Best Practices and elsewhere,[34] NHTSA considers serviceability to be so important that in the Best Practices retain a separate section on the issue that includes the general practice [G.45][35]: "The automotive industry should provide strong vehicle cybersecurity protections that do not unduly restrict access by alternative third-party repair services authorized by the vehicle owner." Providing any party with a particular access or right to vehicle software is outside the scope and intent of this document, even though NHTSA's interest in facilitating serviceability without undue restrictions remains the same. The Best Practices do not hinder industry's ability to facilitate appropriate levels of access to any party while achieving cybersecurity goals.

IV. Economic Analysis for *Cybersecurity Best Practices for the Safety of Modern Vehicles*

NHTSA is finalizing its Cybersecurity Best Practices for the Safety of Modern Vehicles, which is non-binding (i.e., voluntary) guidance provided to serve as a resource for industry on safety-related cybersecurity issues for motor vehicles and motor vehicle equipment. As guidance, the document touches on a wide array of issues related to safety-related cybersecurity practices, and provides recommendations to industry on the following topics: (1) General Cybersecurity Best Practices, (2) Education, (3) Aftermarket/User Owned Devices, (4) Serviceability, and (5) Technical Vehicle Cybersecurity Best Practices.

---

[34]https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/nhtsa_testimony_in_response_to_ma_committee_letter_july_20_2020.pdf

[35] In the draft version, this was G.43.

NHTSA considered the potential benefits and costs that may occur if companies in the automotive industry decide to integrate the recommendations in the Best Practices into their business practices. The following is a summary of the considerations that NHTSA evaluated for purposes of this section.

First, although as guidance the Best Practices is voluntary, NHTSA expects that many entities will conform their practices to the recommendations endorsed by NHTSA. NHTSA believes that the Cybersecurity Best Practices for the Safety of Modern Vehicles serve as means of facilitating common understanding across industry regarding best practices for cybersecurity.

Second, the diversity among the entities to which the Best Practices apply is vast. The recommendations found in Cybersecurity Best Practices for the Safety of Modern Vehicles are necessarily general and flexible enough to be applied to any industry entity, regardless of size or staffing. The recommendations contained within the best practices are intended to be applicable to all individuals and organizations involved in the design, development, manufacture, and assembly of a motor vehicle and its electronic systems and software. These entities include, but are not limited to, small and large volume motor vehicle and motor vehicle equipment designers, suppliers, manufacturers, modifiers, and alterers. NHTSA recognizes that there is a great deal of organizational diversity among the intended audience, resulting in a variety of approaches, organizational sizes, and staffing needs. NHTSA also expects that these entities have varying levels of organizational maturity related to cybersecurity, and varying levels of potential cybersecurity risks. These expectations, combined with NHTSA's lack of detailed knowledge of the organizational maturity and implementation of any recommendations contained within the guidance, make it difficult for NHTSA to develop a reasonable quantification of the per-organization cost of implementing the recommendations.

Third, any costs associated with applying the Best Practices would be limited to the incremental cost of applying the new recommendations included in the document (as opposed to those in the 2016 Best Practices). The updated Cybersecurity Best Practices for the Safety of

Modern Vehicles document highlights a total of 70 enumerated best practices, 21 of which could be considered "new" relative to the first version published in 2016.

Fourth, costs could be limited by organizations who have implemented some of the recommendations prior to this request for comment. NHTSA is unaware of the extent to which various entities have already implemented NHTSA's recommendations, and determining the incremental costs associated with full implementation of the recommendations is effectively impossible without detailed insight into the organizational processes of every company.

Fifth, many of NHTSA's recommendations lean very heavily on industry standards, such as ISO/SAE 21434. Three of the 21 "new" best practices simply reference the ISO/SAE 21434 industry standard. Since many aspects of NHTSA's recommendations are mapped to an industry standard, costs would also be limited for those companies who are adopting ISO/SAE 21434 already. Thus, it would be very difficult to parse whether a company implemented ISO/SAE 21434 or whether it had decided to adopt NHTSA's voluntary recommendations. While the Best Practices have some recommendations[36] that cannot be mapped to an industry standards document at this time, most of those recommendations involve common vehicle engineering and sound business management practices, such as risk assessment and supply-chain management. For these recommendations, NHTSA's inclusion in the Best Practices serve as a reminder.

Regarding benefits, entities that do not implement appropriate cybersecurity measures, like those guided by these recommendations, or other sound controls, face a higher risk of cyberattack or increased exposure in the event of a cyberattack, potentially leading to safety concerns for the public. Implementation of the best practices can, therefore, facilitate "cost prevention" in the sense that failure to adopt appropriate cybersecurity practices could result in other direct or indirect costs to companies (i.e., personal injury, vehicle damage, warranty, recall, or voluntary repair/updates).

---

[36] For example, G.6 in Section 4.2.3 recommends consideration of sensor vulnerabilities as part of risk assessment; and G.10 and G.11 in Section 4.2.6 recommend tracking software components on vehicles in a manner similar to hardware components.

The best practices outlined in this document help organizations measure their residual risks better, particularly the safety risks associated with potential cybersecurity issues in motor vehicles and motor vehicle equipment that they design and manufacture. Further, the document provides a toolset of techniques organizations can utilize commensurate to their measured risks and take appropriate actions to reduce or eliminate them. Doing so could lower the future liabilities these risks represent in terms of safety risks to public and business costs associated with addressing them.

In addition, quantitatively positive externalities have been shown to stem from vehicle safety and security measures (Ayres & Levitt, 1998). The high marginal cost of cybersecurity failures (crashes) extends to third parties. Widely accepted adoption of sound cybersecurity practices limits these potential costs and lessens incentives for attempts at market disruption (i.e., signal manipulation, Global Positioning System (GPS) spoofing, or reverse engineering).

Issued in Washington D.C. under authority delegated in 49 CFR 1.95 and 501.8.

Cem Hatipoglu,

Associate Administrator,

Vehicle Safety Research

[FR Doc. 2022-19507 Filed: 9/8/2022 8:45 am; Publication Date: 9/9/2022]